CLAIMS:

1. (Previously presented) A method of encryption and decryption of data, in which the data is made up of a series of data items, the method including the following steps:

selecting a chaotic equation;

defining starting conditions of the variables of the chaotic equation in the form of an input key; and

applying the chaotic equation to each data item, wherein the method includes an iterate step of updating the chaotic equation and the input key for each iteration value and, in the decryption of data, if a data item is skipped and not received, the method includes applying the iterate step of the chaotic equation for the skipped data item and discarding the result.

2. (Canceled)

3. (Previously presented) A method of encryption and decryption as claimed in claim 1, wherein an updated chaotic equation is applied to each subsequent data item.

4. (Previously presented) A method of encryption and decryption as claimed in claim 1, wherein the step of applying the chaotic equation to the data item includes applying a modular arithmetic operation to combine the real and imaginary parts of the result of the chaotic equation and the data item.

5. (Previously presented) A method of encryption and decryption as claimed in claim 4, wherein the encrypted data item is defined as $v \equiv (v \text{ xor } |z_{n+1}|) \bmod v_{max}$, where z_{n+1} is the value of the chaotic equation and v_{max} is the maximum value of v.

6. (Previously presented) A method of encryption and decryption as claimed in claim 1, wherein the data is a continuous stream of data items.

7. (Previously presented) A method of encryption and decryption as claimed in claim 6, wherein the stream of data items has a rate dependency.

8. (Previously presented) A method of encryption and decryption as claimed in claim 1, wherein the data item is a byte, a word or a dword.

9. (Currently amended) A method of encryption and decryption as claimed in claim 1, wherein the chaotic equation is one of a group that can comprise: Fractal equations, Julia sets, Lorenz attractor, Rossler attractor, ~~Hnon~~ Hénon attractor, Gumowski/Mira attractor and Tinkerbell attractor.

10. (Previously presented) A method of encryption and decryption as claimed in claim 1, wherein the defined variables of the equation are the key to the encryption and are required at the encrypting source and the decrypting receiver.

11. (Canceled)

12. (Previously presented) A method of encryption and decryption as claimed in claim 1, wherein the data items are grouped in blocks with each block having an identifier providing information of the position of the block in the data.

13. (Previously presented) A method of encryption and decryption as claimed in claim 12, wherein the identifier is not encrypted.

14. (Previously presented) A method of encryption and decryption as claimed in claim 12, wherein a mask is generated for each block by applying the chaotic equation to each data item in the block.

15. (Previously presented) An apparatus for encryption and decryption of data, in which the data is made up of a series of data items, the apparatus including:

means for defining a chaotic equation;

means for defining starting conditions of the variables of the chaotic equation in the form of an input key;

means for applying the chaotic equation to each data item; and

an iterate means of updating the chaotic equation and the input key for each iteration value and, in the decryption of data, if a data item is skipped and not received, the iterate means calls the chaotic equation for the skipped data item and discards the result.

16. (Canceled)

17. (Previously presented) An apparatus as claimed in claim 15, wherein the means for applying the chaotic equation to the data item applies an updated chaotic equation to each subsequent data item.

18. (Original) An apparatus as claimed in claim 15, wherein the means for applying the chaotic equation to the data item includes applying a modular arithmetic operation to combine the real and imaginary parts of the result of the chaotic equation and the data item.

19. (Original) An apparatus as claimed in claim 18, wherein the encrypted data item is defined as $v \equiv (v \text{ xor } |z_{n+1}|) \bmod v_{max}$, where z_{n+1} is the value of the chaotic equation and v_{max} is the maximum value of v.

20. (Original) An apparatus as claimed in claim 15, wherein the data is a continuous stream of data items.

21. (Original) An apparatus as claimed in claim 20, wherein the stream of data items has a rate dependency.

22. (Original) An apparatus as claimed in claim 15, wherein the apparatus includes a plurality of defined chaotic equations.

23. (Original) An apparatus as claimed in claim 15, wherein the data item is a byte, a word or a dword.

24. (Original) An apparatus as claimed in claim 15, wherein the chaotic equation is one of a group that can comprise: Fractal equations, Julia sets, Lorenz attractor, Rossler attractor, Henon attractor, Gumowski/Mira attractor and Tinkerbell attractor.

25. (Original) An apparatus as claimed in claim 15, wherein the defined variables of the equation are the key to the encryption and are required at the encrypting source and the decrypting receiver.

26. (Canceled)

27. (Original) An apparatus as claimed in claim 15, wherein the data items are grouped in blocks with each block having an identifier providing information of the position of the block in the data.

28. (Original) An apparatus as claimed in claim 27, wherein the identifier is not encrypted.

29. (Original) An apparatus as claimed in claim 27, wherein a mask is provided for each block by applying the chaotic equation to each data item in the block.

30. (Previously presented) A computer program product stored on a computer readable storage medium, comprising computer readable program code means for performing encryption and decryption of data made up of a series of data items, including for performing the following steps:

selecting a chaotic equation;

defining starting conditions of the variables of the chaotic equation as an input key; and

applying the chaotic equation to each data item, wherein the computer readable program code means further performs an iterate step of updating the chaotic equation and the input key for each iteration value and, in the decryption of data, if a data item is skipped and not received, the computer readable program code means includes applying the iterate step of the chaotic equation for the skipped data item and discarding the result.

31-38. (Canceled)

39. (New) A method as claimed in claim 1, wherein the iterate step of updating the chaotic equation and the input key for each iteration value comprises:

changing the input key to the chaotic equation for each data item in an iterative manner.

40. (New) A method as claimed in claim 1, wherein the iterate step of updating the chaotic equation and the input key for each iteration value comprises:

updating the input key for each iteration value based on a result of an application of the chaotic equation to a data item in a previous iteration.

41. (New) A method as claimed in claim 1, wherein the data item is a byte of data in a stream of data and wherein the input key for the chaotic equation is updated with each byte of data to be encrypted in the stream of data based on an updated chaotic equation, updated based on a previous input key, used to encrypt a previous byte of data in the stream of data.

42. (New) An apparatus as claimed in claim 15, wherein the iterate means of updating the chaotic equation and the input key for each iteration value comprises:

means for changing the input key to the chaotic equation for each data item in an iterative manner.

43. (New) An apparatus as claimed in claim 15, wherein the an iterate means of updating the chaotic equation and the input key for each iteration value comprises:

means for updating the input key for each iteration value based on a result of an application of the chaotic equation to a data item in a previous iteration.

44. (New) An apparatus as claimed in claim 15, wherein the data item is a byte of data in a stream of data and wherein the input key for the chaotic equation is updated with each byte of data to be encrypted in the stream of data based on an updated chaotic equation, updated based on a previous input key, used to encrypt a previous byte of data in the stream of data.

45. (New) A computer program product as claimed in claim 30, wherein the iterate step of updating the chaotic equation and the input key for each iteration value comprises:

changing the input key to the chaotic equation for each data item in an iterative manner.

46. (New) A computer program product as claimed in claim 30, wherein the iterate step of updating the chaotic equation and the input key for each iteration value comprises:

updating the input key for each iteration value based on a result of an application of the chaotic equation to a data item in a previous iteration.

47. (New) A computer program product as claimed in claim 30, wherein the data item is a byte of data in a stream of data and wherein the input key for the chaotic equation is updated with each byte of data to be encrypted in the stream of data based on an updated chaotic equation, updated based on a previous input key, used to encrypt a previous byte of data in the stream of data.